AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method comprising:

maintaining a first page table map for use in an isolated execution mode and a second page table map for use in a normal execution mode;

restricting access to an isolated area of memory to bus cycles performed in the isolated execution mode by a processor operating in the isolation execution mode, the isolated area of memory having ~~a protected~~ an associated audit log to contain hash values representing information that has been successfully loaded into the isolated area of memory ~~preserve fingerprints identifying events being processed in the isolated execution modes~~, the audit log to further act as a fingerprint that identifies the information loaded into the isolated area of memory,~~preserve information associated with the events,~~ the ~~information~~ audit log to further prove ~~proving~~ current status of the isolated execution mode[[~~s~~]];

dynamically swapping between the first page table map and the second page table map responsive to a change in execution mode;

identifying if an event is one of a class of events to be handled in the isolated execution mode;

asserting a selection signal to select the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode; [[and]]

handling the event using a table map selected by the selection signal;

determining if a current mode is the isolated execution mode;

loading a set of control registers with values corresponding to the first page table map if the current mode is not the isolated execution mode and the event is one of the class; and

dispatching an exception vector after the loading is complete.

2. (Previously Presented) The method of claim 1 further comprising:

identifying if the event is one of a class of events to be handled in the isolated execution mode;

handling the event using the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode; and

wherein identifying comprises indexing into a lookup table with a exception vector of the event.

3. (Original) The method of claim 1 wherein dynamically swapping comprises:

loading a set of control registers selected based on an exception vector of the event.

4. (Original) The method of claim 3 wherein the set of control registers comprises:

a global descriptor table register;

an interrupt descriptor table register; and

a page table map base address register.

5. (Original) The method of claim 1 wherein maintaining comprises:

mirroring a page table base address register.

6. (Original) The method of claim 1 further comprising:

defining a set of events that should be handled in isolated execution mode.

7. (Original) The method of claim 6 wherein the set of events to be handled in the isolated execution mode comprises:

machine check events and clock events.

8. (Cancelled)

9. (Currently Amended) An apparatus comprising:

a first storage location storing control data for a first page table map for use in an isolation execution mode;

a second storage location storing control data for a second page table map for use in a normal execution mode;

a selection unit to select which page table map is applied responsive to receipt of an event, the selection unit to dynamically swap between the first page table map and the second page table map responsive to a change in execution mode; and

an isolated execution circuit at a processor to generate isolated access bus cycles to permit the processor to access an isolated area of memory and operate in the isolated execution mode, and further to restrict access to the isolated area, the isolated area of memory having ~~a protected~~ an associated audit log to contain hash values representing information that has been successfully loaded into the isolated area of memory ~~preserve fingerprints identifying events being processed in the isolated execution modes~~, the audit log to further act as a fingerprint that identifies the information loaded into the isolated area of memory,~~preserve information associated with the events,~~ the ~~information~~ audit log to further prove ~~proving~~ current status of the isolated execution mode[[~~s~~]],

wherein isolated access bus cycles are to be used if the apparatus operates in an isolated execution mode.

10. (Original) The apparatus of claim 9 wherein the selection unit comprises:

a multiplexer that selects between the first and the second storage locations based on an exception vector of the event.

11. (Original) The apparatus of claim 9 wherein the first storage location contains a base address for the first page table map and the second storage location contains a base address for the second page table map.

12. (Currently Amended) A computer system comprising:

a processor executing in one of a normal execution mode and an isolated execution mode associated with an isolated area of memory;

a first set of control registers to define a current memory map of the platform;

a mapping unit to dynamically load the first set of control registers responsive to an event if the event should be handled using an alternate memory map, the mapping unit including a second set of registers having a first subset corresponding to control register values for a normal execution mode memory map and a second subset corresponding to control register values for an isolated execution mode memory map, the mapping unit further including a selection unit to select and dynamically swap between the first subset and the second subset, the isolated area of memory having ~~a protected~~ an associated audit log to contain hash values representing information that has been successfully loaded into the isolated area of memory ~~preserve fingerprints identifying events being processed in the isolated execution modes~~, the audit log to further act as a fingerprint that identifies the information loaded into the isolated area of memory,~~preserve information associated with the events,~~ the ~~information~~ audit log to further prove ~~proving~~ current status of the isolated execution mode[[~~s~~]]; and

an isolated execution circuit to generate isolated access bus cycles if the processor is executing in the isolated execution mode, the isolated execution circuit to permit the processor to access the isolated area to operate in the isolated execution mode, and further to restrict access to the isolated area.

13. (Cancelled)

14. (Currently Amended) The computer system of claim [[~~13~~]] 12 wherein the selection unit comprises:

a plurality of multiplexers having selection driven by an exception vector of an incoming event.

15. (Previously Presented) The computer system of claim 12 wherein the first set of control registers comprises:

a global descriptor table register;

an interrupt description table register; and

a page table map base address register.

Claims 16-30 (Cancelled)

31. (Previously Presented) The method of claim 1, wherein the isolated area being accessible by the processor operating in the isolation execution mode via an isolated execution circuitry at the processor, and wherein restricting access includes protecting the isolated area by access checks, and permitting access to the isolated area via special bus cycles issued by a processor.

32. (Currently Amended) A non-transitory processor readable medium comprising instructions that when executed, cause a machine to:

maintain a first page table map for use in an isolated execution mode and a second page table map for use in a normal execution mode;

restrict access to an isolated area of memory to bus cycles performed in the isolated execution mode by a processor operating in the isolation execution mode, the isolated area of memory having ~~a protected~~ an associated audit log to contain hash values representing information that has been successfully loaded into the isolated area of memory ~~preserve fingerprints identifying events being processed in the isolated execution modes~~, the audit log to further act as a fingerprint that identifies the information loaded into the isolated area of memory,~~preserve information associated with the events,~~ the ~~information~~ audit log to further prove ~~proving~~ current status of the isolated execution mode[[~~s~~]];

dynamically swap between the first page table map and the second page table map responsive to a change in execution mode;

identify if an event is one of a class of events to be handled in the isolated execution mode;

assert a selection signal to select the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode; [[and]]

handle the event using a table map selected by the selection signal;

determine if a current mode is the isolated execution mode;

load a set of control registers with values corresponding to the first page table map if the current mode is not the isolated execution mode and the event is one of the class; and

dispatch an exception vector after the load is complete.

33. (Previously Presented) The processor readable medium of claim 32 wherein the instructions that when executed, further cause the machine to:

identify if the event is one of a class of events to be handled in the isolated execution mode;

handle the event using the first page table map if the event is identified as one of the class of events to be handled in the isolated execution mode; and

wherein identifying comprises indexing into a lookup table with a exception vector of the event.

34. (Previously Presented) The processor readable medium of claim 32 wherein the instructions that when executed to dynamically swap, cause the machine to:

load a set of control registers selected based on an exception vector of the event.

35. (Previously Presented) The processor readable medium of claim 34 wherein the set of control registers comprises:

a global descriptor table register;

an interrupt descriptor table register; and

a page table map base address register.